TekResults Newsletter (April 2023)

To unsubscribe send an email to UnsubscribeNewsletter@tekresults.com with unsubscribe to Newsletter in the subject line or click here UnsubscribeNewsletter@tekresults.com

Dear Clients and Friends

Spring is upon us! Time to put away the winter clothes and snow shovels and break out the tanning lotion. Ok, so it's April and that might be a bit optimistic, but it doesn't hurt to hope! We have some great stuff for you in this edition of the newsletter. so let's get started!

In this newsletter

- Backing up your email
- Protecting your critical systems
- Four of our favorite features in the Windows 11 February update
- Outlook 365's redesigned interface
- Windows 11 advertisement scare

Computer sale!

With Windows 10 quickly approaching the end of its supported life, now is an excellent time to replace those aging computers. We have many desktops and laptops in stock to help make your holidays bright! We specialize in refurbished Dell systems that look great and come nicely appointed with a solid state drive, at least 16GB memory and an Intel Core i5 or i7 processor. We bench test each of our systems to ensure they are working in top-notch order before presenting them for sale, and each one comes with our 30-day warranty. Most of our systems feature Windows 11 Pro, but we still have a few Windows 10 systems in stock – priced to sell. Drop us a line and we can help you find just the right system to put under your tree.

Referrals

TekResults owes much of its success to our loyal and enthusiastic clients. It's those of you who tell your friends about us that keep our company growing, and we'd like to say thanks. Just telling someone about us is all it takes. Just let us know you dropped our name, and we'll drop a gift card in the mail. See, who said talk is cheap!

Businesses Who Need Our Referrals

Any business who has slow computer systems
Any business who has slow network
Any business needing a better disaster recovery strategy including backups for mission-critical devices (servers, essential PCs, etc.), equipment redundancy,
Any business requiring help upgrading existing IT infrastructure due to obsolescence
Any business that needs better email services

Any business that needs to migrate to a new software platform
Any business that needs help with its industry vertical market software
Any business that has employees and compliance questions
Any business that needs help with employees working from home
Any business that needs reliable IT service
Any business that is purchasing another business and needs IT help
Any business that is being sold or is being dissolved
Any business with human resource issues as they pertain to IT
Any business that wants to save money and improve functionality by utilizing a VoIP Business phone systems
Any business needing a better security infrastructure
Any business needing remote desktop applications
Any business needing help migrating to Microsoft 365
Any business that would benefit from monitoring of performance, security, etc. of their IT infrastructure
Any business that would like an IT department that will visit and report on each device on a scheduled basis
Any business that would like to read our newsletter or other mail tips and blasts

Backing up your email

Organizations continue to choose Microsoft 365 for ease of collaboration in the cloud. Today, Microsoft 365 is at [300 million commercial seats](#) and growing. Pretty impressive. And we'd like to think Microsoft has guaranteed that all those email mailboxes are safe from loss. Well, not so fast, my friend; we should look at the fine print.

The fine print in this instance is in the form of [Microsoft's Shared Responsibility Model](#) (MSRM). In a nutshell, when you subscribe to Microsoft 365, you are agreeing to participate in the MSRM, which means you agree that Microsoft will be responsible for THEIR global infrastructure and their commitment to keeping their infrastructure up and running, consistently delivering uptime reliability of their cloud services. YOUR responsibility is to have complete access and control of your data — regardless of where it resides. This also means protecting the data from loss. To put a finer point on it, if Microsoft loses your data they can, potentially, tell you that backing up your data was YOUR responsibility. Also if someone in your organization makes a mistake and inadvertently deletes important data or does it maliciously or (god forbid) if someone breaks in and launches a ransomware attack then Microsoft will help with recovery but does not guarantee that they will be able to recover.

Replication vs Backup

For their part, Microsoft delivers a solid infrastructure and reliable cloud services that include built-in data replication; this provides data center to data center georedundancy. This replication is a necessity. If something goes wrong at one of Microsoft's global data centers, they can failover to their replication target, and in most cases, the users are completely oblivious to any change.

But replication isn't a backup. And furthermore, this replica isn't even YOUR replica; it's Microsoft's. So, what's the difference between a replica and a backup anyhow? A backup is commonly defined as a separate copy of data that's stored in a separate location, from which data can quickly and easily be recovered. Data replication is the process of storing the same data in multiple locations.

While having a replica of your data may sound similar to having a backup of your data, it's important to note that with a replicated copy, all data is copied, whether it was deleted or corrupted, meaning you now have a copy of all good data and all bad data, and as we mentioned, this is Microsoft's data and it's use is not guaranteed to you. Thus, relying solely on Microsoft to maintain and host your data puts your organization at risk of losing control and access to your own company's data.

How to protect your data from loss

The counter to putting Microsoft in the position of sole protector of your data is to protect the data yourself. When we talk about data here, we include your email, OneDrive documents, Teams data and everything you have stored in

SharePoint. In short, everything you have stored on Microsoft's 365 servers. There are various third-party solutions that will make the backup process easy, but before we get to that, let's look at some other great reasons to back up your email.

7 Reasons to back up your email

Veem Software, a data protection company, has identified 7 Reasons Why Microsoft 365 Backup is Critical

1. **Accidental deletion:** This is actually the most common cause of data loss in Microsoft 365. If you delete a user, whether you meant to or not, that deletion will then be replicated across the network. A backup (yours – not Microsoft's) could restore that user, either to on-premises Exchange or Microsoft 365.
2. **Retention policy gaps and confusion:** Retention policies in Microsoft 365 are designed to help organizations comply with regulations, laws and internal policies that require that they retain or delete content; they are not backups. But even if you do rely on your retention policy in place of a backup, these retention policies are hard to keep up with, let alone manage. A backup provides longer and more accessible retention that's all protected and stored in one place for easy recovery.
3. **Internal security threats:** When we think of threats to our business, we usually think in terms of protecting against external forces. However, many businesses also experience threats from the inside, and these issues happen more often than you think. Having a high-grade recovery solution mitigates the risk of critical data being lost or destroyed.
4. **External security threats:** Ransomware is becoming more and more sophisticated, and criminals are finding more ways to reach our users and deceive them into clicking a link that encrypts the entire organization's data for ransom. A backup can easily restore data to an instance before the attack.
5. **Legal and compliance requirements:** There are eDiscovery capabilities built into Microsoft 365, but a third-party backup solution is purposely built to easily search within a backup and quickly bring back data to meet any regulatory compliance needs.
6. **Managing hybrid email deployments and migrations to Microsoft 365:** Whether you are migrating to Microsoft 365 or have a blend of on-premises Exchange and Microsoft 365 users, the exchange data should be managed and protected the same way, which makes the source location irrelevant.

How to back up your email and 365 data

Many of our TekResults clients back up their servers and other mission critical computers every night, however these backups only back up things that are stored on the computer. Those things usually do not include email. An email backup at the office level wouldn't do you any good if Microsoft were to lose your data. Why? Because Outlook stores your email in an OST file. These files can be backed up, but when you restore them to another computer from the backup, they won't work. Outlook requires a connection to the 365 Exchange servers to keep your mailbox up to date and if Outlook finds an old version of the OST file, it won't use it.

Fortunately, there are cloud-based solutions dedicated to email backup. Microsoft has its own backup solution, but you guessed it, it's not free. At TekResults, we rely on Cloud-to-Cloud Backup, a Zix-AppRiver solution. Zix-AppRiver is the service provider we use for all our email clients, so we already have a relationship with them should you decide to use their 365 backup solution.

Carbonite Cloud-to-Cloud Backup provides a comprehensive solution to protect your cloud applications and data and offers these features.

- Automate backups of Microsoft 365
- Protect against ransomware, malware, data loss and data breach
- Flexibly search and recover items, mailboxes or sites at any granular level
- Easily recover data with point-in-time recovery
- Browse daily snapshots and run searches
- Feel more secure with full redundancy
- Store more with unlimited storage and retention

To get started, or just to ask some questions, give us a call. We'd love to discuss this with you.

Protecting your critical systems

In every office, there are always one or more computers that, should they break, would bring company productivity to a grinding halt. Until these *mission-critical systems* can be repaired quickly, they can represent lost revenue or lost productivity. For that reason, it's important to have a safety net for when things go wrong.

It makes sense that your sever is probably the most important system in your business and you have probably taken great care to ensure that your server is backed up regularly, but what about those individual workstations that use specific software to keep your business going? Here are a couple examples.

Several of our clients use FedEx shipping manager to keep track of the many products they ship. Some of our other clients use UPS WorldShip to perform a similar job. In most cases, the FedEx and UPS software are installed on a specific workstation in the shipping department. That workstation is used to store the shipping database and to manage day-to-day shipping operations. If this workstation goes down, the entire shipping operation comes to a halt.

We have several clients who work with highly specialized programs to help them do research and development. These programs take time to install, and the installation process usually requires someone from the software manufacturer's support team to assist. In other words, reinstalling the software is a pain and cannot be done quickly. If the shipping computer goes down, shipping comes to a stop until the computer can be repaired.

If a catastrophic system failure occurs it is usually caused by either a motherboard failure or a hard drive failure. If the motherboard fails, in many cases the hard drive (containing all the vital stuff) can simply be moved to a similar workstation. However if the hard drive fails, restoration may not be so simple.

For several years, we have been recommending that these mission-critical systems should be backed up using software that creates an image, or snapshot of the computer, and we still strongly recommend this. There is also another way you can protect yourself from disaster, by replacing your computer with a system that has redundancy built into it. Here's how it works.

Most servers are built containing two or more hard drives that are configured in what's called a RAID configuration. RAID (redundant array of independent disks) is a way of storing the same data in different places on multiple hard disks or solid-state drives (SSDs) to protect data in the case of a drive failure. If one hard drive fails, the other RAID disk, containing the same data, takes over, thus minimizing or eliminating down time.

RAID Storage vs. Data Backup
While RAID can make your data storage more powerful and resilient, it's not the same thing as regular data backup. RAID arrays spread I/O operations across multiple disks in order to read and write data faster, or to mirror data on one drive across other drives, which allows the whole system to continue operating without data loss if one of those drives fails.

On the other hand, data backup helps you restore lost files. So, while data backup solutions are meant to get you back on your feet in the event of total data loss, RAID is designed to help avoid that kind of loss in the first place. Similarly, while RAID makes your overall storage system more resilient, it still only counts as one copy of your data.

This leads to the question, which do I need. In most cases we absolutely recommend backing up your system regularly, but in those situations where you can't afford to be without your system for any period of time, there's no reason you can't do both. A Raid system can be backed up as easily as a non-RAID system. We recommend this approach.

Where to get a RAID system

RAID isn't just for servers. There are workstations available with this option as well. TekResults has some reasonably priced Dell RAID systems in stock, ready to deploy. Give us a call to discuss and we will be happy to assist in finding the best solution for you.

Four of our favorite features in the Windows 11 February 2023 Update

The Windows 11 February 2023 update brought with it some excellent features that can really enrich how you use the operating system. Here are a few of our favorites.

Record your screen with the Snipping Tool
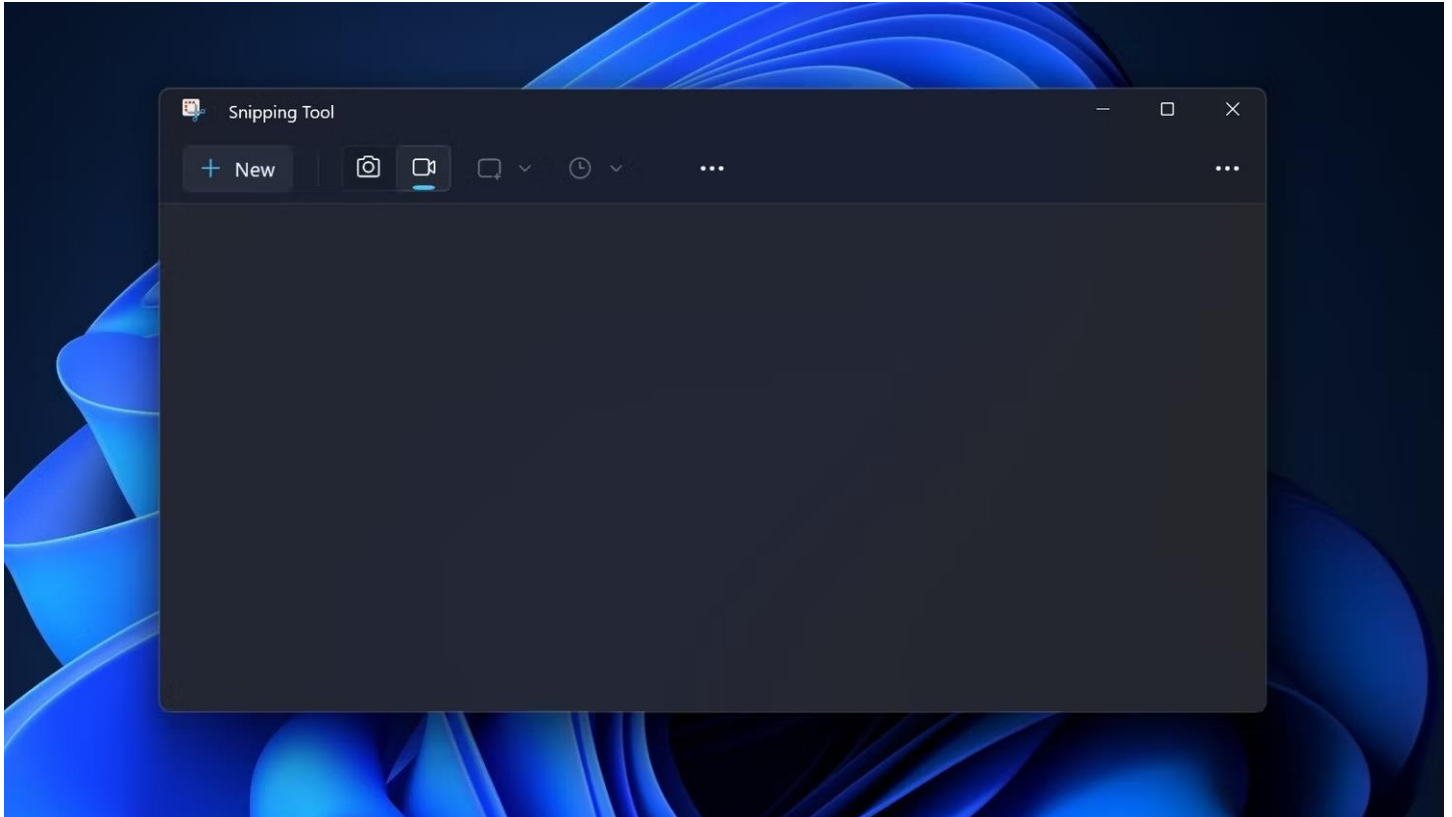
Before the arrival of the Windows 11 February 2023 update, users were primarily dependent on third-party tools like Snag-It or Camtasia to capture what was happening on their PC screens. But now, the new Snipping Tool can also start a recording session of what is happening on your PC screen.

You can select a portion of your screen before starting the session. Also, you can pause or resume the recording whenever you like. However, screen recording in Snipping Tool will only record what is going on your screen, not the audio.

You can click the Start button on the Taskbar and type "Snipping Tool," and then press **Enter** on your keyboard to open the app. To start a screen recording session, click the **video cam** icon and click **New**.

A tabbed interface in notepad
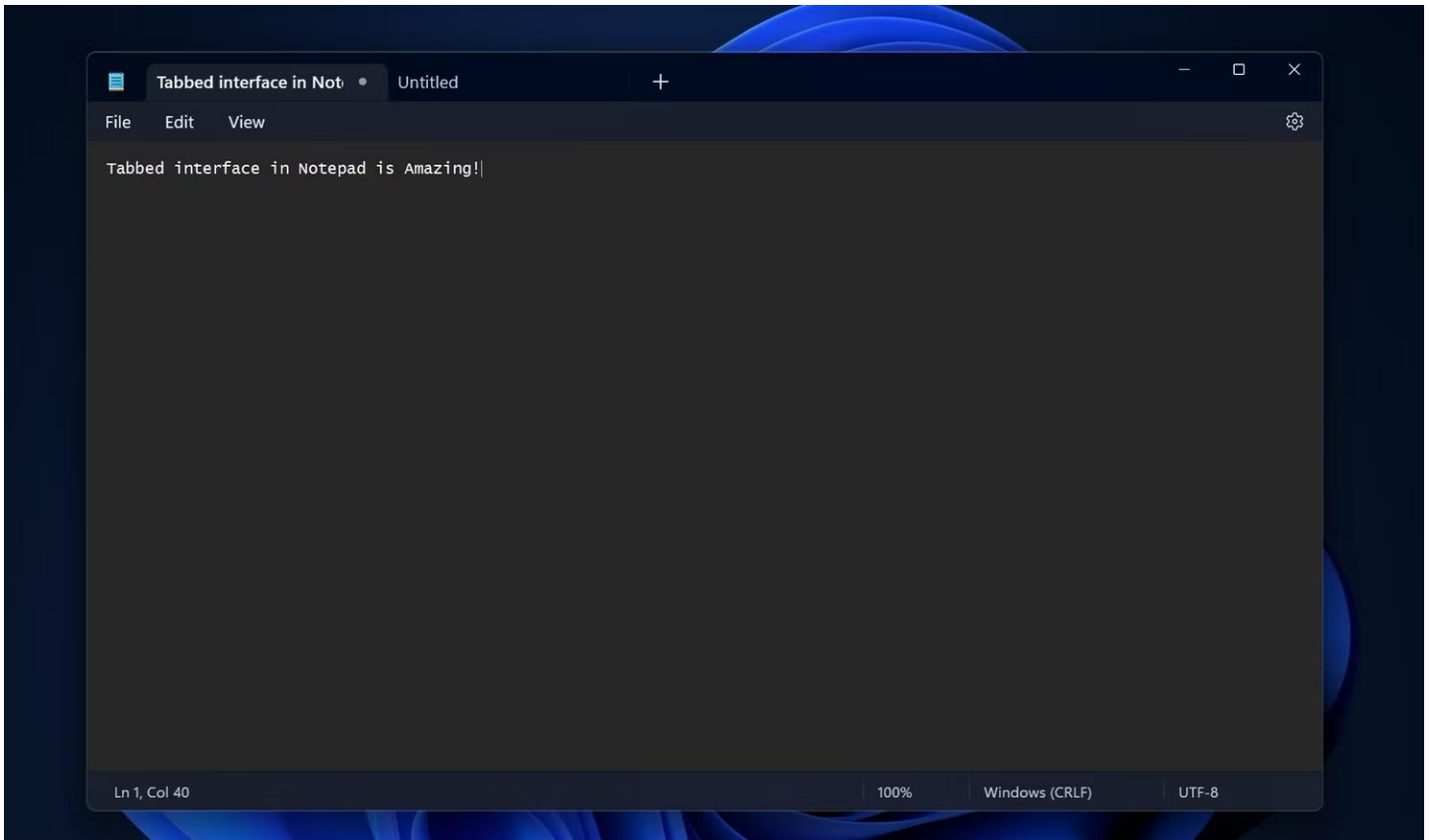
The tabbed interface is now expanded to the Notepad. Like in File Explorer, the new Notepad will enable you to open multiple folders and directories in one app window. Because different folders or directories can be in a single Notepad window due to the tabs support, it is easier for you to switch between them.

If you are not seeing tabs in Notepad after upgrading to the February 2023 update, go to Microsoft Store and get the latest version of the app.

New designs for the search bar in the taskbar
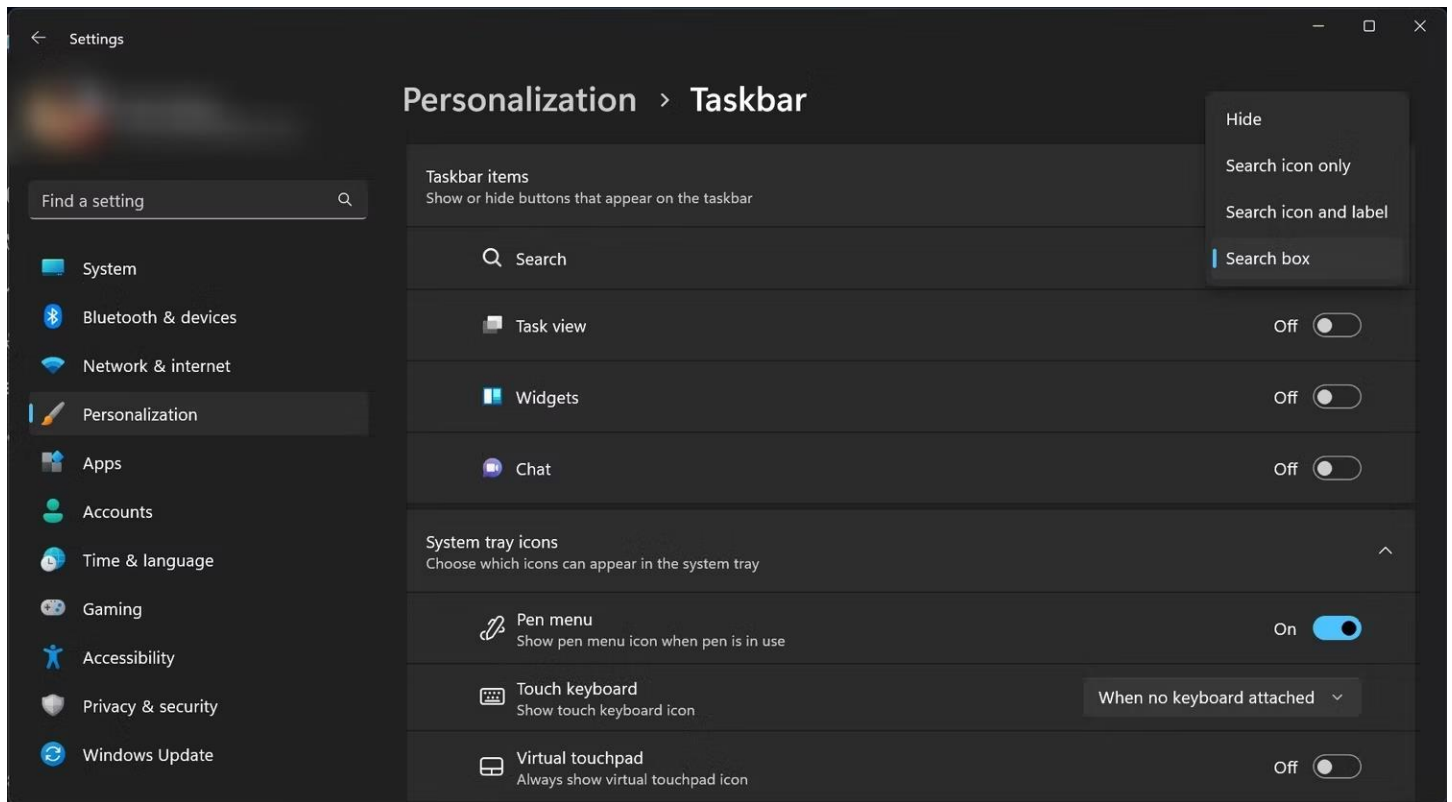
You can finally change the design of Search on the Windows 11 Taskbar after installing the February 2023 update. Three different design options exist for the Taskbar Search: **Search icon only, Search icon with label**, and **Search box**.

Among the three design options, the last one will occupy the most space in Taskbar. The ability to hide Search from appearing in Taskbar is also there. If you need more help, check out how to get started with Windows 11 Taskbar Search.

Search for processes or tasks in task manager
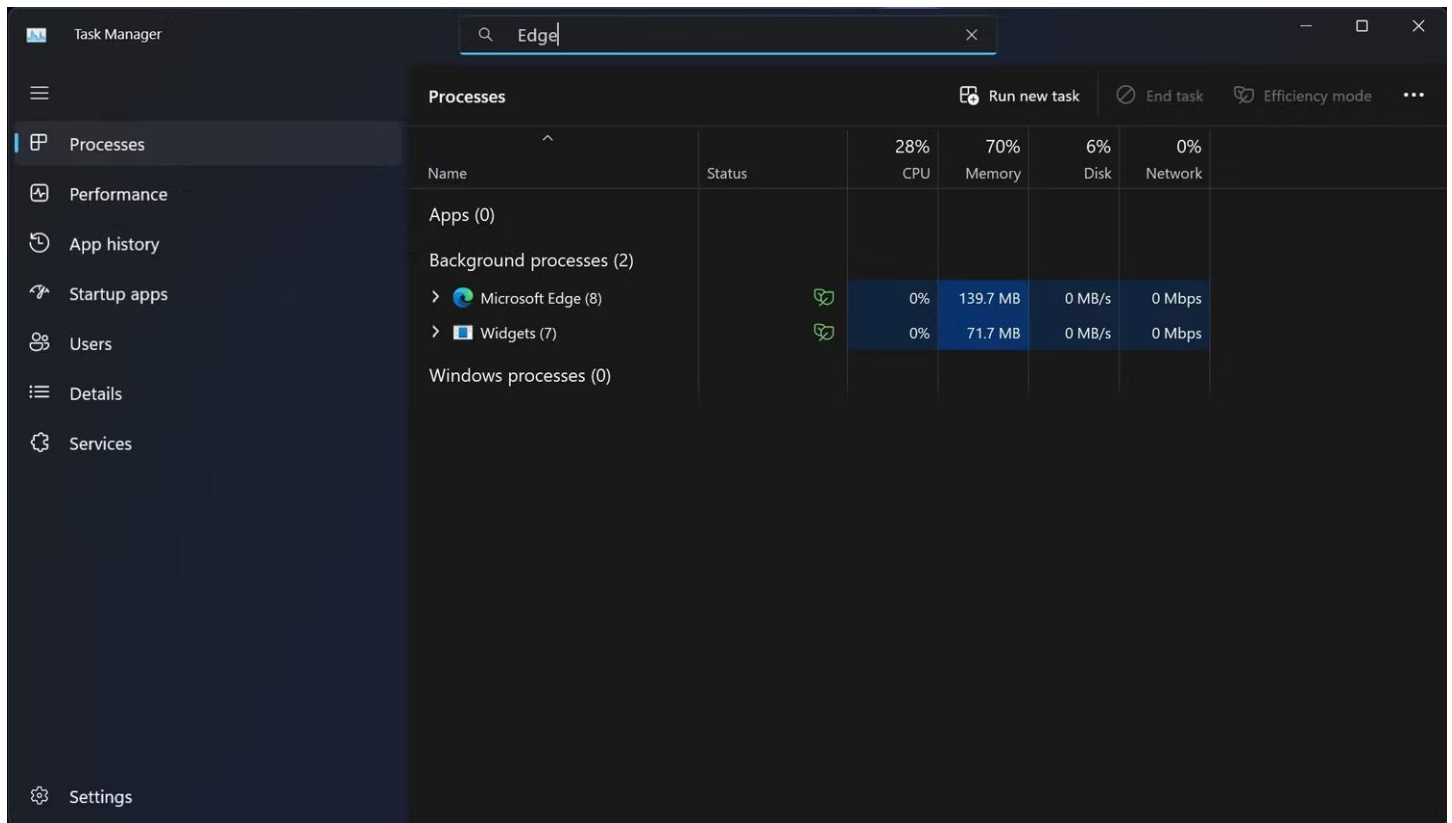
Before the February 2023 update, there was no search functionality in Task Manager. As a result, users could not find the task or process quickly. The February feature drop fixes the issue by introducing a search strip at the very top of the Task Manager.

If for some reason, you want to check what's happening with a particular task or process, you can easily find it by using the search strip instead of scrolling through the bottom to spot it in Task Manager. After successfully installing the February 2023 update, you should immediately see the search functionality in the Task Manager, as it is enabled by default.

To open the Task Manager, right-click on the Taskbar and select **Task Manager**. If you are not familiar with it, check out how to use Windows Task Manager.

Outlook 365's redesigned interface

You may have noticed that Outlook has a new look. Some users have asked why the modules that used to appear at the bottom of the navigation pane now appear at the top left.
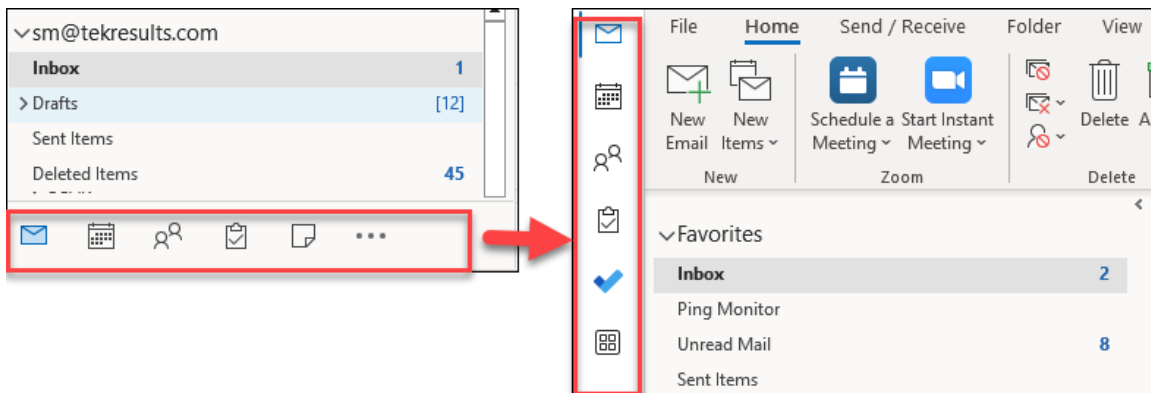
:
This update is a step towards a consistent experience across apps like Outlook, Teams, and Office.com. From the new location, you can switch apps and it creates room in the UI for more apps to integrate with Outlook. You can easily launch popular apps like To Do, Yammer, Bookings, Word, Excel, and PowerPoint without leaving Outlook, with more to come. Currently, only Microsoft apps such as Yammer, To Do and Bookings are available to users.

For those of you who would like to put things back the way they were, here's how to do it.

1. In Outlook, Click on File > Options > Advanced.
2. Uncheck the box next to **Show Apps in Outlook**.
3. Restart Outlook.
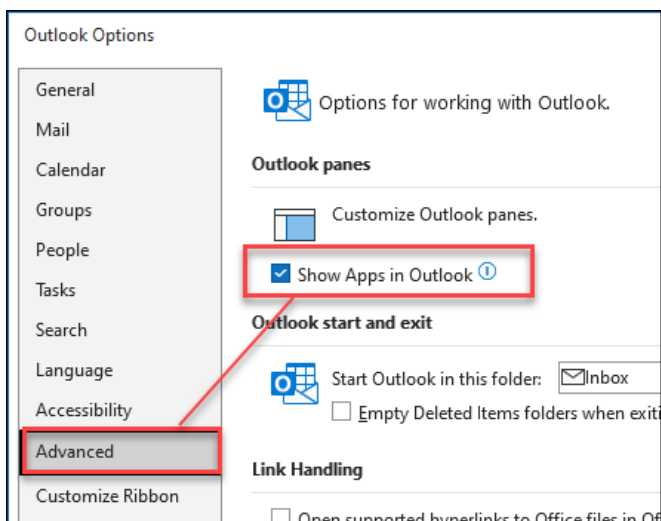
Windows 11 advertisement scare

Recently we've received calls from Windows 10 clients who report they are locked out of their computers and they think their system is infected with a virus. After investigating, we discovered that what they had was a full screen advertisement from Microsoft, encouraging them to upgrade to Windows 11. Unfortunately, Microsoft didn't make it obvious how to dismiss the message without actually upgrading.

If you see this message, before hitting the panic button, here are some things to try if you don't want to upgrade now.

− Click **Keep Windows 10** in the bottom left of the window.
− In some cases, we've found clicking the link didn't do anything (thanks Microsoft). In this case you need to sign out. No, there's no option in the window to do that, so you will have to press **Ctrl+Alt+Del** on the keyboard to bring up a window with options, one of which is **Sign out**.

- After signing out, sign back in again with your username and password. When the annoying offer appears again, click **Keep Windows 10**. It should work this time, but that won't be the end of it.
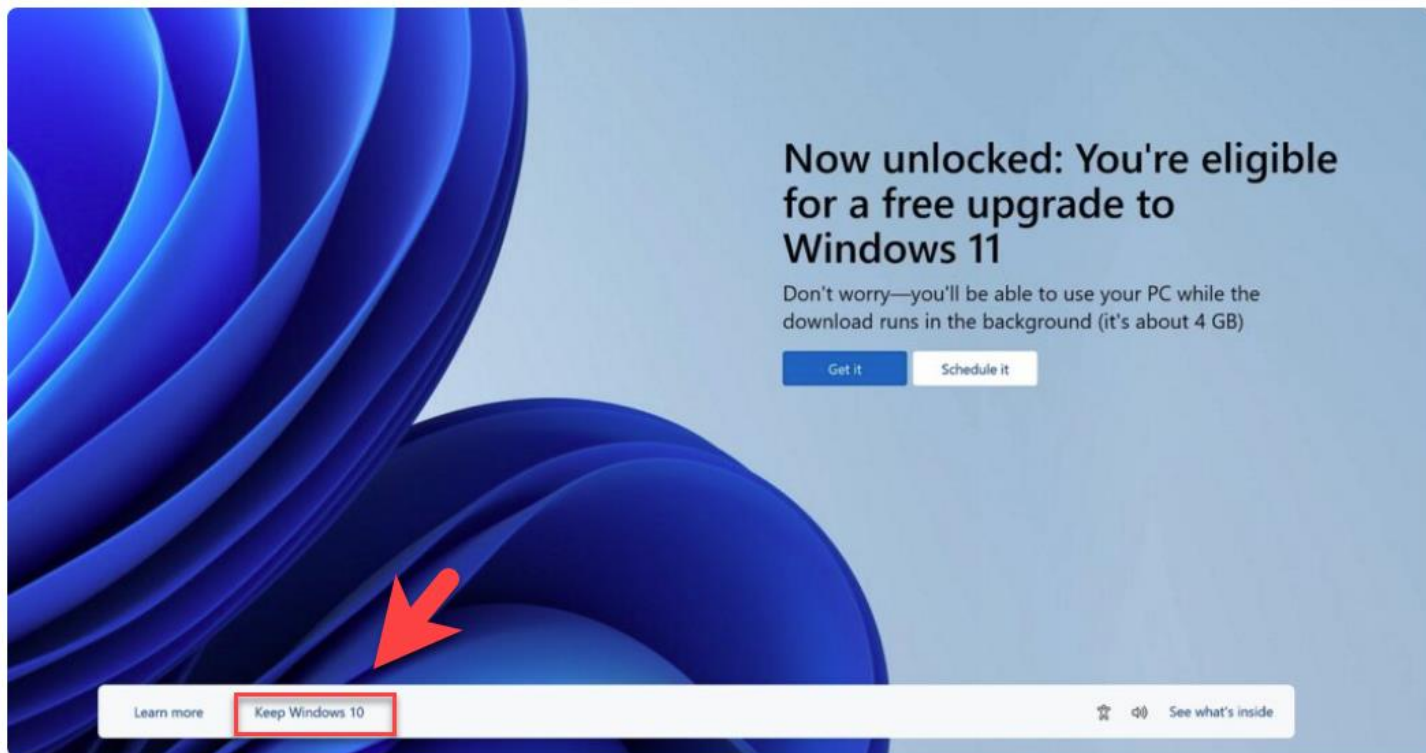
Clicking the option won't take you back to the desktop. Instead, it will open another page titled *Introducing Windows 11*, which highlights several features you can use after upgrading. You can click the **back** button, but it again won't close the Windows 11 upgrade screen.

The back button opens another window titled *Microsoft recommends Windows 11 for your PC*. Click **Decline upgrade**.

And finally, you get to the last screen, *You'll stay on Windows 10*. Click **Continue to Windows 10**.
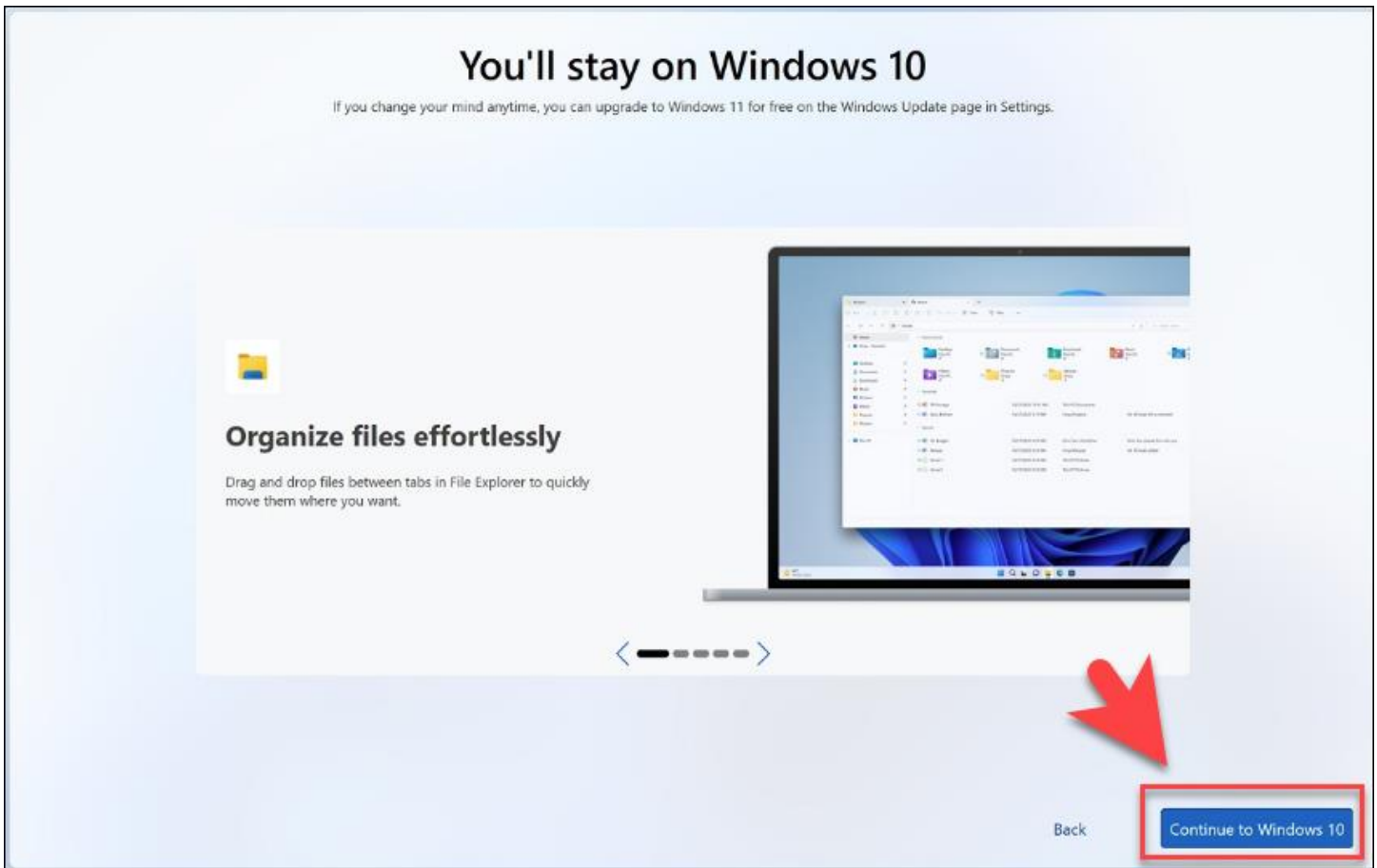
That should do it. Unfortunately, there's no way to bypass these alerts and they can reappear in future.

If you need help, please call us.

Martin A.Sheridan
TekResults Ltd.
P.O. Box 95,
Pine Grove Mills, PA 16868
Work: 814-206-0000 x101
Mobile: 814-207-4323
mas@tekresults.com
www.tekresults.com
TekResults... Your complete IT partner